NOISY BYZANTINE AGREEMENT IN QUANTUM NETWORKS

Alexandru-Andrei Cîrjaliu-Davidescu
A.A.Cirjaliu-Davidescu@student.tudelft.nl
TU Delft – CSE3000 Research Project
Supervisor & Responsible Prof.: Tim Coopmans

IMPACT OF GATE ERRORS ON A WEAK BROADCAST PROTOCOL

1. BACKGROUND

- **Byzantine Agreement** = Major challenge in distributed computing: achieving consensus in a multi-party communication, even in the presence of malicious parties[1].
- **Weak Broadcast Protocol** - WBC(3,1)[2] = Quantum implementation of a 3-party Byzantine Agreement. Uses a 4-qubit entangled quantum state and a classical communication channel. Structured into 4 phases.
- **Linear Circuit** = Circuit implementation[2] of the WBC.
- Problem: Quantum circuits are very susceptible to **noise**.

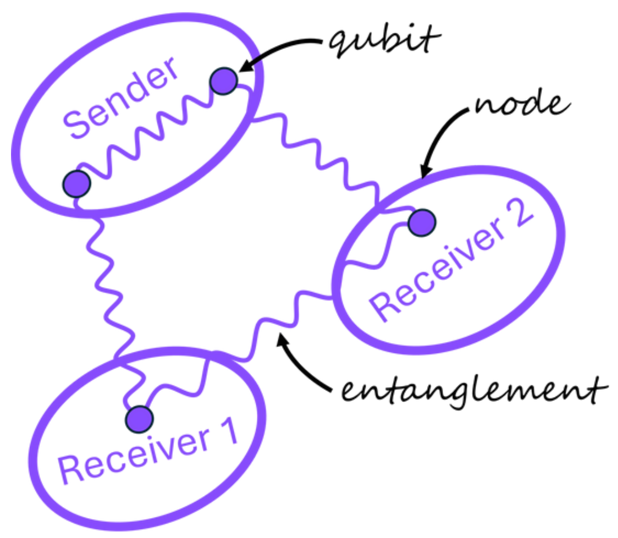


Figure 1: Representation of the state

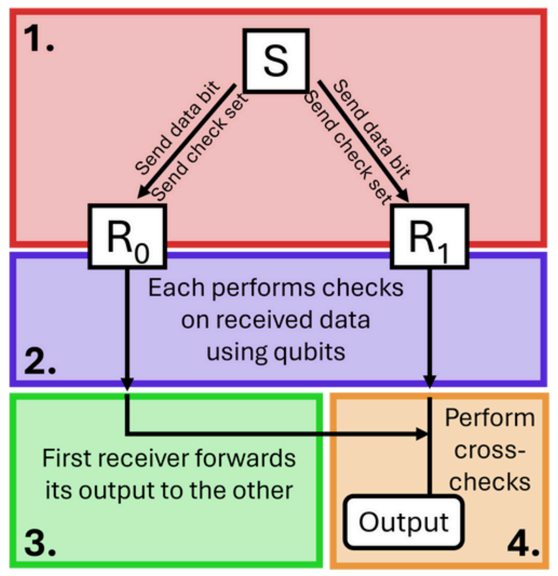


Figure 2: Protocol Phases

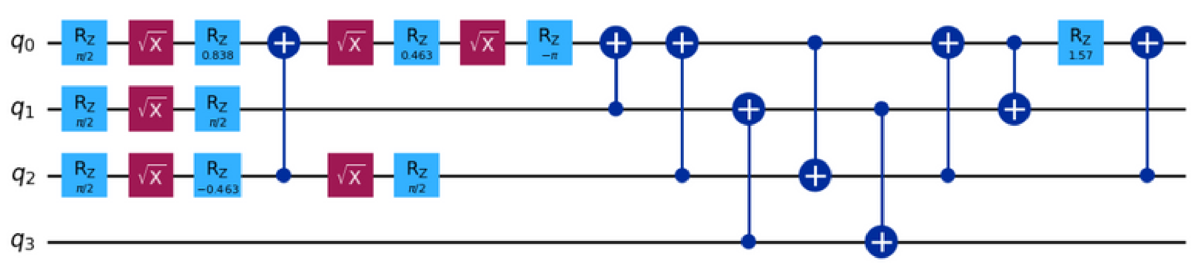


Figure 3: Linear Circuit Diagram

2. OBJECTIVES

Research topic: "*How does **gate-level depolarizing noise** affect the WBC(3,1) protocol in a quantum simulation?*"

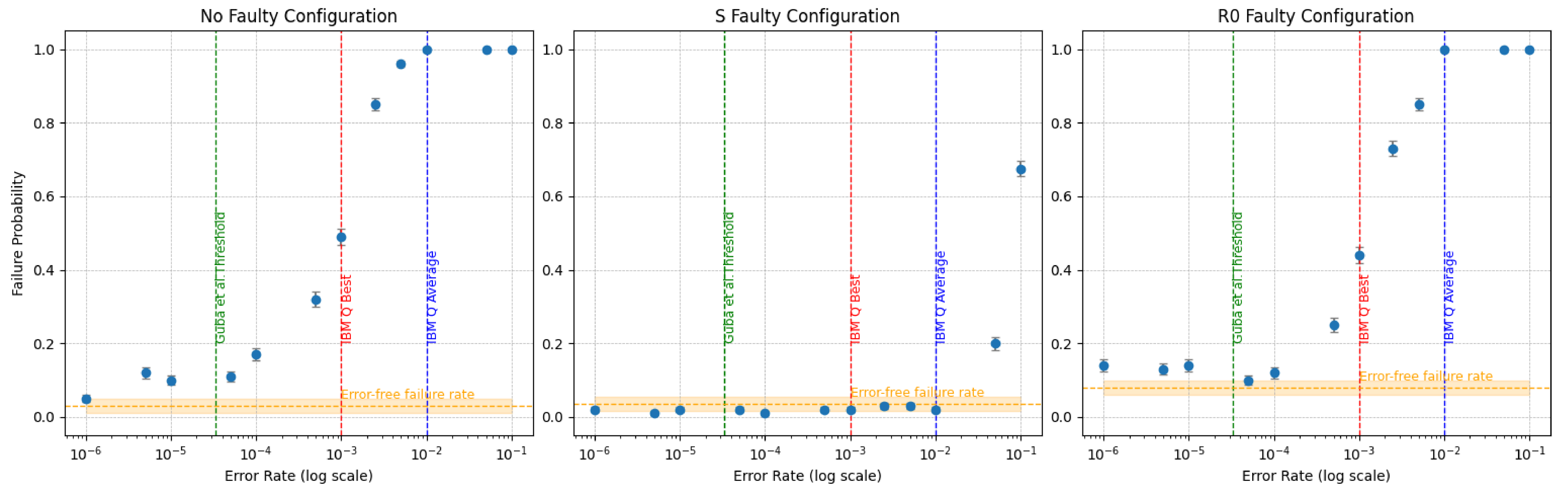
- Investigate the impact of depolarizing gate-level noise[3] on the Linear Circuit implementation of the WBC.
- Evaluate protocol failure probability under different noise levels and adversary models, and evaluate how the probability of protocol failure varies as a function of noise.
- Find noise thresholds at which the WBC becomes unreliable for practical use, and compare those thresholds to existing rates on contemporary hardware.

3. METHODOLOGY

- Simulated the Linear Circuit using SquidASM[4] and NetSquid[5].
- Applied depolarizing noise to 2-qubit gates in the circuit, isolating impact and excluding preparation or measurement noise.
- Tested under three adversary configurations:
  - no faulty - all parties are honest, and transmit their true values
  - sender (S) faulty - sender sends different data to each receiver
  - 1st receiver (R0) faulty - manipulates data forwarded to the second receiver to make them output a specific result

4. KEY FINDINGS

- Visual Plots: Failure Probability (y-axis) vs. Noise Level Rate (x-axis, visualized in log scale). Plots also present error bars, error-free failure rates, and various noise thresholds present in contemporary research or hardware.
- Noise has impact even at low levels. Failure increases non-linearly with noise.
- Clear thresholds identified for no faulty and R0 faulty configurations:
  - Protocol fails often (consistently in no faulty and R0 faulty) at ~1% noise.
  - Sharp increase in failure rates at noise levels of 0.1% and 1%.
- S Faulty case shows more robustness compared to other configurations, but also fails with high probability at noise levels above 1%.



5. ANALYSIS

- WBC(3,1) is sensitive to even modest levels of gate noise.
- Failure rates rise sharply at noise levels as low as 0.001, with near-total failure at 0.01, values closely aligned with real-world quantum hardware[6]. Therefore, implementation on real hardware does not yet seem viable.
- S faulty's greater robustness highlights asymmetry in adversarial models.

6. RECOMMENDATIONS

Future work should explore:

- Alternative noise models, such as measurement errors.
- Error mitigation strategies applied to the protocol.
- Investigating protocol redesigns, such as adaptive thresholds.

7. CONCLUSION

This study evaluated the impact of gate-level depolarizing noise on the Linear Circuit implementation of the WBC(3,1) Weak Broadcast Protocol proposed by Guba et al[2].

The key finding is that noise levels commonly found on today's quantum devices render the protocol unreliable, especially in honest scenarios.

The simulations expose an important limitation: the protocol is not currently deployable without error mitigation. These results stress the need for hardware-aware protocol design in quantum networking.

[1] Leslie Lamport et al., *The byzantine generals problem*. ACM Trans. Program. Lang. Syst., July 1982.
[2] Zoltan Guba et al., *Resource analysis for quantum-aided byzantine agreement with the four-qubit singlet state*. Quantum, 2024.
[3] M. M. Wilde, *Quantum Information Theory*. Cambridge University Press, 2007.
[4] QuTech. *Squidasm: A modular quantum network simulator interface*. Available: https://github.com/QuTech-Delft/squidasm
[5] QuTech. *Netsquid - network simulator for quantum information using discrete events*. Available: https://netsquid.org/
[6] IBM Quantum, *Quantum processing units*. Available: https://quantum.ibm.com/services/resources.